

MeetingPlace Web with DMZ Onsite Installation

Document ID: 60133

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Items to Verify Before You Go Onsite

- Verify Connectivity
- Click to Attend Considerations

Items to Verify Before You Start Onsite Work

- Verify Connectivity
- Group Default Set in MeetingTime
- MeetingPlace Web Installation

Items to Verify After Onsite Work

- Test Public Meetings
- Test Meetings
- Test Lecture–Style Meetings
- Web Conferencing and Notification Verification

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document outlines verification procedures for use before you go onsite, or before you start onsite work, and after you have completed any Cisco MeetingPlace Web with Demilitarized Zone (DMZ) onsite work.

Prerequisites

Requirements

Confirm you have read the Cisco MeetingPlace Web Release Notes Release 5.3 and the requirements are met. Different deployment model requirements, Segmented Meeting Access–1 Server (SMA–1S) and Segmented Meeting Access–2 Server (SMA–2S) are found on pages six and seven of the release notes document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco MeetingPlace Web version 5.3
- DMZ Architecture (DMZ–B and DMZ–C) (These are referred to as SMA–1S and SMA–2S in the Administrator's Guide for Cisco MeetingPlace Web Conferencing Release 5.3 Setup and Configuration.)

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Items to Verify Before You Go Onsite

This section outlines verification steps necessary before you go onsite.

Verify Connectivity

Complete these steps:

1. Review Chapter 5 in the Administrator's Guide for Cisco MeetingPlace Web Conferencing Release 5.3 regarding how to configure External web conferencing, along with the Secure Socket Layer (SSL) setup.
2. Verify that port 80 or port 443 (SSL protocol) is open from the Internet and to DMZ server.
3. Verify that port 80 is open from the intranet and to the Internet.
4. Verify that port 5003 is open between the DMZ server and the Cisco MeetingPlace server (Cisco MeetingPlace Gateway System Integrity Module [GWSIM] uses this).
 - ◆ Initiated from the DMZ server to the intranet
5. For WebShare, make sure you have port 1627 open from the Internet and to the DMZ server if you want to avoid tunneling.
 - ◆ Initiated from the Internet to the DMZ server
 - ◆ If this port is not open, then tunneling through port 80 or 443 is used, which is ten percent slower.
6. For WebShare, make sure that you have port 1627 open from the intranet and to the DMZ server if you want to avoid tunneling.
 - ◆ Initiated from the intranet to the DMZ server
 - ◆ If this port is not open, then tunneling through port 80 or 443 is used, which is ten percent slower.
7. For NetMeeting only, verify that you have port 1503 open from the Internet and to the DMZ server.
 - ◆ Initiated from the Internet to the DMZ server
8. For NetMeeting only, verify that you have port 1503 open from the intranet and to the DMZ server.
 - ◆ Initiated from the intranet to the DMZ server

Click to Attend Considerations

Consider these factors:

1. Can a segmented (or split) Domain Name System (DNS) be used? This allows you to use a single URL in your notifications.
2. If not, you must decide how to modify the notification templates:
 - ◆ Do you plan to use two URLs?
 - ◆ Do you plan to use a different URL based on whether the meeting is public or private?
3. Confirm whether you have a pilot of end users to test functionality after the install or upgrade.
4. Do you use or plan to use NT Authentication?

Items to Verify Before You Start Onsite Work

Verify Connectivity

Complete these steps:

1. Ping and NSLOOKUP (if open) the fully qualified domain name (FQDN) or IP address of the internal Web server from another internal PC.
 - ◆ Ping meetingplace.company.com (replace with the correct hostname of the server)
 - ◆ NSLOOKUP meetingplace.company.com (replace with the correct hostname of the server)

Note: To use NSLOOKUP, open a DOS prompt (go to **Start > Run**, enter **cmd** and click **OK**), then enter **NSLOOKUP meetingplace.company.com** (replace with the correct hostname of the server).
2. Ping and NSLOOKUP (if open) the FQDN or IP address of the DMZ Web server from an external PC.
3. Ping and NSLOOKUP (if open) the FQDN or IP address of the DMZ Web server from another internal PC.
4. Ping and NSLOOKUP (if open) the FQDN or IP address of the MeetingPlace server from the DMZ Web server.
5. Telnet on port 5003 from the DMZ Web server to the Cisco MeetingPlace server. Follow these steps to confirm that the port is open:
 - a. Go to **Start > Run** and enter the **telnet servername 5003** command, where *servername* is the name or IP address of the MeetingPlace server, and click **OK**.
 - b. If you see a series of nonsensical characters (for example, :¶e;4/v \?V \?ÿø), port 5003 is open.
 - c. Enter **Ctrl-]** (Control, right bracket) to exit.
 - d. If you get a failed connection, as shown here, then port 5003 is not open:

```
Could not open connection to the host, on port 5003: Connection
failed
```

Group Default Set in MeetingTime

What are the most common types of scheduled meetings?

Note: If the scheduled meetings are mostly internal, set the group default Display Meeting to Everyone feature to **No**. If they are mostly public meetings, then set Display Meeting to Everyone to **Yes**.

MeetingPlace Web Installation

Complete these steps (these steps vary based on whether they apply to a one- or two-server deployment):

1. Verify the hardware and software requirements for the servers.

Makes sure that the hardware on the gateway machine meets all of the appropriate requirements. The machine that hosts more conferences must have the faster, better hardware.
2. For SMA-1S deployment, follow the steps for implementation in Table 5-1, and for Segmented Meeting Access for 2 Server Deployment, refer to Table 5-2 in the Administrator's Guide for Cisco MeetingPlace Web Conferencing Release 5.3.

Items to Verify After Onsite Work

Test Public Meetings

Verify these items:

1. Verify these abilities:

- ◆ Use the internal web site to login as a profiled user.
- ◆ To schedule a public meeting, use the internal web site.
- ◆ To schedule a public meeting with an attachment, use the internal web site.
- ◆ You can view attachments from an internal PC.
- ◆ You receive the notifications for the above meeting.
- ◆ The Click to attend link works internally.
- ◆ The Click to attend link works from an Internet PC.
- ◆ Internal and the external viewers can join the web conference, as well as share and collaborate in the same web conference.

2. Confirm these abilities and restrictions on the external site:

- a. You are logged in as your profile when you attend from the internal site.
- b. You can access the attachments and slide show from the external server.
- c. Guests cannot add attachments or change permissions or user display options.

Note: If the meeting room appears to be frozen at one percent or if the meeting room features are grayed out, the hostname may be input incorrectly or the DMZ template is not currently used for external meeting redirect.

Test Meetings

Complete these verification steps.

1. Verify these abilities:

- a. You can schedule a private meeting from the internal web site.
- b. You can view this private meeting from an internal PC.
- c. You can schedule a private meeting with an attachment from the internal web site.
- d. You can view attachments from an internal PC.
- e. You receive the notifications for the above meeting.
- f. The Click to attend link works internally.
- g. The internal viewers can join the Web conference.

2. Verify these restrictions:

- a. You cannot attend a private meeting from the DMZ web site.
- b. You are not redirected to the DMZ web site when you join the Web conference.

Test Lecture–Style Meetings

Complete these verification steps.

1. Verify these abilities:

- a. You can schedule both a public and a private lecture–style meeting from the intranet.
- b. A profiled user can host a lecture–style meeting from the intranet and the Internet.
- c. A profiled user is allowed to collaborate from the intranet and the Internet.

2. Verify these guest restrictions:

- a. A guest cannot host a lecture–style meeting from the intranet.
- b. A guest cannot host a lecture–style meeting from the Internet.
- c. A guest is not allowed to collaborate from the intranet.
- d. A guest is not allowed to collaborate from the Internet.

Web Conferencing and Notification Verification

Complete these verification steps.

1. To verify tunneling if port 1627 is not open:
 - a. Login to the Web Admin user interface (UI).
 - a. Log in to **Cisco MeetingPlace Web**.
 - b. The **Admin** link is at the top right of the Welcome page.
 - b. Click the **Data Conferencing Server** link.
 - c. Click the **Advanced** link.
 - d. Check the **Force HTTP tunneling** box.
 - e. Click the **Join Web Conference** button.
 - f. If the WebShare client opens ("Welcome to MeetingPlace Application Sharing."), tunneling is functional.
 - g. If the WebShare client does not open, tunneling is not functional. You should contact Cisco Technical Support.
2. Verify that the notification is sent out correctly and that the Click to attend link works.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Voice
Service Providers: Voice over IP
Voice & Video: Voice over IP
Voice & Video: IP Telephony
Voice & Video: IP Phone Services for End Users
Voice & Video: Unified Communications
Voice & Video: IP Phone Services for Developers
Voice & Video: General

Related Information

- **Cisco MeetingPlace Web Conferencing System Manager s Guide**
- **DMZ Info site**
- **Voice Technology Support**
- **Voice and Unified Communications Product Support**
- **Recommended Reading: Troubleshooting Cisco IP Telephony**
- **Technical Support & Documentation – Cisco Systems**

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Aug 09, 2006

Document ID: 60133
